DEPARTMENT OF THE ARMY
Headquarters, Engineer Brigade, 1st Armored Division
Unit 24141
APO AE 09169

COMMAND POLICY

POLICY NUMBER: 6-19	Proponent: AETV-THQ-SI	Date: 1 November 2005

SUBJECT: Command Policy Memorandum, Automation Security

REFERENCE: a. DOD 5500.7-R, Joint Ethics Regulation, SECDEF.
b. AR 25-1, The Army Information Resources Management Program.
c. AR 25-11, Record Communications and the Privacy Communications System.
d. AR 25-55, The Department of the Army Freedom of Information Act Program.
e. AR 380-19, Information Systems Security.
f. USAREUR Reg. 25-1, USAREUR Information Management Program.
g. USAREUR Email Policy Memorandum 2 July 97.
h. 1st Armored Division Policy Statement 6-1.

PURPOSE: To layout the guidelines for Automation Security

1. As the 1st Armored Division Engineer Brigade continues to modernize, advancements in information technology continue to improve efficiency. The benefits of information systems such as electronic mail (e-mail) have led to our increased dependence on automated communications. This dependence requires an increased level of responsibility throughout the command to prevent abuse of these systems and to protect users from security risks associated with their use.

2. To prepare for this new way of doing business, controls must be in place to ensure that new technology and increased communications capabilities support command-and-control requirements and general administrative needs. The enclosed policy provides these controls. The effectiveness of this policy, however, depends on individual and organizational compliance.

3. To ensure that e-mail and the Internet serve the best interests of their organization, this command, and the U.S. Army, leaders must ensure that all military and civilian personnel comply with this policy. Doing so will help ensure that we can accomplish our current missions as efficiently as possible while laying the foundation for how we do business in the 21st century.

4. POC is the 1st Armored Division Engineer Brigade Signal Officer at DSN 343-9447.

DEPARTMENT OF THE ARMY
Headquarters, Engineer Brigade, 1st Armored Division
Unit 24141
APO AE 09169

COMMAND POLICY

IRON SAPPERS!

1. Encl.
    1. 1st AD EN BDE Automation Policy

//ORIGINAL SIGNED//
JAMES D. SHUMWAY
COL, EN
Commanding

DISTRIBUTION:
CDR, HHD, EN BDE
CDR, 502ND EN CO
CDR, 526TH EN DET
CDR, 518TH EN DET

ENCLOSURE 1

1st Armored Division Engineer Brigade
Automation Policy

1. Purpose. The purpose of this memorandum is to prescribe 1st Armored Division Engineer Brigade policy and procedures for using Government-provided electronic mail (e-mail) systems and for using the Internet.

2. Applicability. This policy applies to 1st Armored Division Engineer Brigade commands and Engineer Brigade Staff Offices.

3. Responsibilities.

a. Commanders. Commanders are responsible for--

(1) Implementing and enforcing this policy.

(2) Controlling access to and use of Internet services.

b. Information Assurance Managers (IAMs). Each IAM is responsible for--

(1) Ensuring that information systems security requirements are met according to regulations in the 25 and 380 series. These requirements govern sending, receiving, processing, and storing electronically transmitted information.

(2) Implementing comprehensive anti-virus-protection procedures and maintaining close oversight of the virus-protection program.

(3) Verifying that all accreditations are complete, accurate, and current. Accreditations must correspond to existing equipment, hardware, and software.

c. Information Management Officers (IMOs). Each IMO is responsible for--

(1) Coordinating with IAMs to ensure that functional and operational requirements are met according to security guidelines.

(2) Ensuring the efficient use of information systems in their assigned areas of responsibility.

d. Systems Administrators. Each SA is responsible for--

(1) Providing for and overseeing technical operations that support e-mail.

(2) Ensuring that systems-security requirements are applied to their assigned e-mail systems, local area network (LAN), and Internet connections in coordination with servicing security personnel.

(3) Maintaining and managing a password and log-in control program.

(4) Establishing and maintaining group address lists.

(5) Managing the assignment and establishment of e-mail addresses and associated mailboxes.

4. Policy. E-mail and the Internet may be used only for official and authorized purposes. The policy in this enclosure governs official and authorized use and is published in USAREUR Regulation 25-22.

a. Security.

(1) E-mail transmissions must follow security and privacy restrictions (AR 25-55, AR 340-21, and AR 380-19).

(2) Classified and unclassified-sensitive information is not authorized on nonsecure common-user e-mail systems according to AR 380-5 and AR 380-19. Classified and unclassified-sensitive e-mail may be sent and received only on systems and networks that are secure and accredited at the security level of the information. Unclassified-sensitive information is information that the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or conduct of Federal programs; or the privacy to which individuals are entitled under the Privacy Act.

b. Fraud, Waste, Abuse, and Ethics. E-mail must be used only to conduct official Government business and for other authorized purposes. Any other use of e-mail systems, networks, or services will be considered fraud, waste, or abuse. All violations will be reported through the Battalion/ Brigade IAM to the Unit Commander for appropriate action. The following are examples of information that is not authorized for transmission through organizational or individual e-mail:

(1) Information that advertises or publicizes individual or non-Government groups, organizations, companies, or activities that may gain a financial or competitive advantage or increased prestige. This does not include events cosponsored by Government-commercial contractors when these events are requested by and are of benefit to the Government.

(2) Obscene or sexually explicit information, such as pornography or other illegal material.

(3) Personal announcements or advertisements for the sale or solicitation of goods or services

for personal gain.

(4) Chain mail. Recipients of chain letters will delete them and not forward or respond to them. Users should be especially alert for chain letters that try to elicit sympathy for an individual or a cause.

NOTE: The directive governing ethics (DOD 5500.7-R) is punitive. DOD 5500.7-R, paragraph 2-301, prescribes DOD-wide limitations on e-mail use. Violators of these limitations may be subject to Uniform Code of Military Justice action or adverse administrative action (for example, nonjudicial punishment, reprimand, fine, suspension, employment termination).

c. Authorized Personal Use. Government e-mail systems and networks are authorized for personal use for morale and welfare (MW) purposes. Commanders must determine what MW purposes are appropriate and reasonable within the context of their operational mission, available resources, and security requirements and ensure that subordinate supervisors are informed of this determination. In making this determination, commanders must ensure that personal use of e-mail--

(1) Does not adversely affect the performance of duty of the individual using e-mail for MW or of anyone else in the organization (for example, ensuring that personal use does not prevent a time-sensitive, mission-related message from being sent).

(2) Is limited to reasonable amounts of time.

(3) Is individually controlled by deleting personal messages (both sent and received) or downloading them onto a diskette as soon as practical.

(4) Is limited to personal, non-duty time, when possible. In determining when authorized use is possible during personal, non-duty time, approval authorities may consider individual mission requirements, differences in time zones, personal emergencies, and other such factors.

(5) Does not result in significant cost to the Government in terms of time, equipment, or other resources associated with personal use (for example, supplies and storage capacities).

(6) Does not require existing equipment, systems, or networks (for example, hardware, software, telecommunications connectivity) to be expanded, extended, or upgraded.

(7) Meets security considerations and requirements based on the system and equipment used (for example, operations; personnel; physical security; system accreditation; virus checks, protection, and tests).

(8) Serves a legitimate public interest (for example, keeping employees in their workplace

rather then requiring them to leave to use a commercial or private system, educating and training personnel, improving the morale of personnel deployed for 30 or more days).

(9) Does not adversely reflect on the U.S. Government, DOD, DA, or USAREUR.

d. Monitoring.

(1) DOD computer systems may be monitored by authorized personnel to--

(a) Ensure use is authorized.

(b) Manage the system.

(c) Ensure protection against unauthorized access.

(d) Verify security procedures.

(2) Monitoring includes "hacker" attacks to test or verify system security against use by unauthorized persons. During testing and verification, information stored on the system may be examined, copied, and used for authorized purposes, and the data or programs may be placed on the system. The information individual users place on the system therefore is not private.

(3) Use of DOD computer systems, authorized or unauthorized, constitutes consent to official monitoring of the system. Unauthorized use of a DOD computer system may result in criminal prosecution. Evidence of unauthorized use collected during monitoring may be given to appropriate personnel for administrative, criminal, or other official adverse actions.

e. Receiving And Forwarding Unauthorized E-Mail

(1) Receiving. Receipt of e-mail is not controllable. Most Army e-mail systems interconnect with other Government and private sector e-mail systems. If unauthorized or illegal e-mail is received, the recipient is responsible for deleting, destroying, reporting, or otherwise properly disposing of the e-mail to ensure it does not remain on the system.

(2) Forwarding. Forwarding unauthorized or illegal e-mail violates Army e-mail policy, even if the person forwarding the e-mail is not the originator. The individual who receives e-mail, whether sent to an individual or organizational e-mail address, is responsible for ensuring that only authorized and approved e-mail is forwarded.

f. Internet.

(1) General. Government systems such as e-mail can be used to gain access to the Internet.

The Internet is a global communications system shared by individual, Government, non-Government, foreign, academic, industrial, commercial, and other networks. The Internet provides access to a virtually unlimited number of information resources, such as the World Wide Web (memorandum, HQ USAREUR/7A, AEAPA, 31 Mar 97, subject: USAREUR World Wide Web Homepage and Website Policy).

(2) Government Use. The Internet may be used to meet day-to-day operational requirements.

(3) Personal Use. Reading or downloading information from the Internet for unofficial or for other than authorized personal use is strictly prohibited and will be considered abuse of the system. Limited personal use of the Internet may be authorized under the same provisions that apply to use of e-mail.

(4) Security.

(a) The Internet is global and diverse. This increases the risk of security problems. Connection to the Internet not only gives users access to everyone else on the Internet, everyone else on the Internet has access to the user. Using the Internet therefore increases vulnerability to system disruption, unauthorized entry, and computer viruses.

(b) Because of the increased risk to security caused by connection to the Internet, security-accreditation requirements and operations-security procedures must be followed. Anti-virus protection and virus-checker software must be used.

(5) Commercial Internet Chat Sites. Under no circumstance are users authorized to download, install or operate software for the purpose of conducting Commercial Internet Chat. Commercial Internet Chat Sites are a prime targeting tool for hackers who have exploited the chat connections that military users establish in order to infiltrate military networks. Because of the threat to the military networks represented by Commercial Internet Chat, 5th Signal Command will block Commercial Internet Chat sites and services. Legitimate military chat is provided by the Army Knowledge Online website.